TỘI PHẠM MẠNG, TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO, CHỨNG CỨ ĐIỆN TỬ VÀ NHỮNG VẤN ĐỀ ĐẶT RA ĐỐI VỚI HOẠT ĐỘNG ĐÀO TẠO NGÀNH LUẬT NGÀNH LUẬT TRONG CÁC TRƯỜNG ĐẠI HỌC Ở VIỆT NAM HIỆN NAY

Nguyễn Đức Hạnh[(1)]
(1) Trường Đại học Kiểm sát Hà Nội
Ngày nhận bài 25/10/2024; Chấp nhận đăng 25/11/2024
Liên hệ email: hanhtrangvnncs@gmail.com

Tóm tắt

Trong thập kỷ gần đây, sự bùng nổ của công nghệ thông tin và trí tuệ nhân tạo (AI) đã mở ra nhiều cơ hội nhưng cũng đồng thời tạo ra những thách thức lớn, đặc biệt là trong lĩnh vực an ninh mạng tại Việt Nam. Theo báo cáo của Bộ Công an Việt Nam, trong năm 2022, số vụ tội phạm mạng đã tăng lên 3.000 vụ, tăng 20% so với năm trước. Điều này cho thấy tội phạm mạng đang trở thành một vấn đề cấp bách mà xã hội phải đối mặt. Các hình thức tội phạm phổ biến bao gồm lừa đảo trực tuyến, tấn công mạng vào hệ thống thông tin và đánh cắp dữ liệu cá nhân. Sự gia tăng này không chỉ gây thiệt hại về tài chính mà còn ảnh hưởng đến niềm tin của người tiêu dùng và doanh nghiệp vào môi trường trực tuyến. Bài viết này tập trung nghiên cứu: (1) tổng quan tội phạm mạng, tội phạm sử dụng công nghệ cao và chứng cứ điện tử, chỉ ra các đặc điểm và nhấn mạnh tới việc phân loại tội phạm mạng, tội phạm sử dụng công nghệ cao; (2) nghiên cứu chứng cứ điện tử trong việc phát hiện và xử tội phạm mạng, tội phạm công nghệ cao. Từ đó phân tích, dự báo một số thách thức hiện nay liên quan đến tội phạm mạng, tội phạm công nghệ cao và đề xuất một số gợi ý cho hoạt động đào tạo ngành luật trong các trường đại học ở Việt Nam trước những thách thức liên quan đến tội phạm mạng, tội phạm công nghệ cao hiện nay.

Từ khoá: *chứng cứ điện tử, tội phạm mạng, tội phạm sử dụng công nghệ cao*

Abstract

CYBERCRIME, HIGH-TECH CRIME, ELECTRONIC EVIDENCE, AND CHALLENGES FOR LEGAL EDUCATION IN VIETNAMESE UNIVERSITIES TODAY

Over recent decades, rapid advancements in information technology and artificial intelligence (AI) have brought both significant opportunities and serious challenges, especially in the field of cybersecurity in Vietnam. According to a 2022 report by Vietnam's Ministry of Public Security, the number of cybercrime cases rose to 3,000, marking a 20% increase from the previous year. This growth underscores the urgency of addressing cybercrime as a pressing social issue. Common types of cybercrime include online fraud, attacks on information systems, and personal data theft. These activities not only cause financial losses but also erode consumer and business trust in digital environments. This article will (1) provide an overview of cybercrime, high-tech crimes, and electronic evidence, examining their characteristics and categorization, and (2) explore the role of

electronic evidence in detecting and combating cybercrime and high-tech offenses. Based on this analysis, it will also assess current challenges in addressing cybercrime and propose recommendations for enhancing legal education in Vietnamese universities to better respond to these issues.

1. Tội phạm mạng và tội phạm sử dụng công nghệ cao

1.1. Khái niệm về tội phạm mạng và tội phạm sử dụng công nghệ cao

Tội phạm mạng là một khái niệm hiện nay đã được dùng tương đối phổ biến trong đời sống xã hội. Ở một nghĩa chung nhất tội phạm mạng có thể được hiểu là một hành vi vi phạm pháp luật, được thực hiện bằng cách sử dụng công nghệ thông tin và truyền thông (ICT) để nhắm mục tiêu vào các mạng, hệ thống, dữ liệu, trang web hoặc thông qua các công nghệ thông tin và truyền thông (ICT) tạo tiền đề, điều kiện để thực hiện hành vi phạm tội (Goodman, Marc D. and Brenner, Susan W. 2002; Wall, David, 2007; Wilson, Clay, 2008; International Telecommunication Union (ITU), 2012; Maras, Marie-Helen, 2014, 2016).

Khoản 7 Điều 2 Luật an ninh mạng năm 2018 có đưa ra khái niệm: *"Tội phạm mạng"* đó là là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

Theo khoản 1 Điều 3 Luật Công nghệ cao năm 2008 thì: *"Công nghệ cao là công nghệ có hàm lượng cao về nghiên cứu khoa học và phát triển công nghệ; được tích hợp từ thành tựu khoa học và công nghệ hiện đại; tạo ra sản phẩm có chất lượng, tính năng vượt trội, giá trị gia tăng cao, thân thiện với môi trường; có vai trò quan trọng đối với việc hình thành ngành sản xuất, dịch vụ mới hoặc hiện đại hóa ngành sản xuất dịch vụ hiện có".*

Ngày 07/4/2014 Thủ tướng Chính phủ đã ban hành Nghị định số 25/2014/NĐ-CP (Nghị định số 25 của Chính phủ) quy định về phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao và đã quy định: *"Trong Nghị định này, công nghệ cao bao gồm công nghệ thông tin và viễn thông"* (khoản 2 Điều 1). Theo đó, tại khoản 1 Điều 3 của Nghị định này quy định: *"Tội phạm có sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật hình sự có sử dụng công nghệ cao".*

– Theo BLHS năm 1995 của Australia và Phần 10.7 của Luật Thịnh vượng chung (Commonwealth legislatim - Part 10.7 Computer Offences) thì tội phạm công nghệ cao được hiểu là *"Sự xâm nhập máy tính một cách trái phép, sự sửa đổi trái phép dữ liệu bao gồm việc phá hủy dữ liệu, tấn công từ chối dịch vụ (DOS); tấn công từ chối dịch vụ phân tán (DDOS); có sử dụng botrets tạo ra và phân phối phần mềm độc hại".*

– Theo từ điển Luật học Black's law, tội phạm máy tính (Computer crimnal) được hiểu là *"Tội phạm đòi hỏi kiến thức về công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện tội phạm"*.

– Tại cuộc họp lần thứ 10 ngày 27/10/2000 của Đại hội đồng Liên hợp quốc tổ chức tại thành phố Viên (Thủ đô nước Áo) có hội thảo và bàn về ngăn chặn, xử lý tội phạm công nghệ cao đã đưa ra khái niệm tội phạm này theo hai hướng:

+ Tội phạm công nghệ thông tin theo nghĩa hẹp là *"những tội phạm có hành vi sử dụng máy tính cũng như mạng lưới Internet để xâm phạm đến an toàn của hệ thống máy tính và các dữ liệu lưu trữ của hệ thống đó, gây ảnh hưởng, thiệt hại cho người dùng được gọi là tội phạm công nghệ cao"*;

+ Tội phạm công nghệ thông tin được hiểu theo nghĩa rộng là *"những tội phạm có hành vi sử dụng máy tính cũng như sử dụng các phương thức khác có liên quan đến máy tính, mạng máy tính để thực hiện các hành vi lừa đảo, trốn thuế, mạo danh gây ra những mối đe dọa, làm sai lệch thông tin ảnh hưởng đến người dùng được gọi là tội phạm công nghệ cao"*.

Ngoài ra, theo Công ước của Hội đồng châu Âu về Tội phạm mạng (Công ước Budapest) năm 2001: Tội phạm mạng còn được hiểu là những hành vi truy cập, cản trở bất hợp pháp việc truyền tải dữ liệu máy tính, can thiệp trái phép dữ liệu, sử dụng trái phép thiết bị, giả mạo, lừa đảo liên quan đến máy tính, vi phạm liên quan đến hình ảnh, khiêu dâm trẻ em, vi phạm quyền tác giả và quyền liên quan qua hệ thống máy tính,…

Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là tội phạm sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ ở trình độ cao và được thực hiện trên không gian mạng nhằm tác động trái pháp luật đến thông tin, dữ liệu, tín hiệu được lưu trữ, xử lý, truyền tải trong hệ thống mạng máy tính, mạng viễn thông, thiết bị số, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân.

Như vậy có thể khẳng định tội phạm mạng chính là một dạng tội phạm phổ biến và cơ bản của công nghệ cao. Ngoài ra công nghệ cao còn bao gồm: công nghệ sinh học phân tử, công nghệ vật liệu, công nghệ hóa học, công nghệ điện toán đám mây, trí tuệ nhân tạo (AI) Internet kết nối vạn vật (IoT)…

1.2. Đặc điểm của tội phạm mạng và tội phạm sử dụng công nghệ cao

Tội phạm mạng có những đặc điểm khác với tội phạm truyền thống ở chỗ:

– Tội phạm mạng không bị giới hạn bởi ranh giới địa lý hoặc vật lý.

– Tội phạm mạng khi thực hiện thường dễ dàng hơn, nhanh hơn và mất ít công sức thực hiện hơn so với tội phạm truyền thống.

– Để thực hiện được tội phạm mạng thì bắt buộc phải có máy tính, mạng máy tính, các hình thức công nghệ truyền thông thông tin khác làm công cụ, phương tiện thực hiện tội phạm.

– Để thực hiện được tội phạm mạng thì bắt buộc phải thông qua không gian mạng, sử dụng Internet, công nghệ kỹ thuật số, các yếu tố này như là một phương thức giúp cho tội phạm được thực hiện cho dù nó là tội phạm truyền thống hay tội phạm tấn công trực tiếp vào mạng máy tính, mạng viễn thông. Điều đó có nghĩa vai trò của công nghệ thông tin và truyền thông (ICT) đối với hành vi phạm tội là hết sức quan trọng. Công nghệ thông tin và truyền thông (ICT) có thể là mục tiêu của hành vi phạm tội nhưng cũng có thể là phương thức để thực hiện tội phạm. Khi ICT là mục tiêu của hành vi phạm tội, tính nguy hiểm của hành vi phạm tội gây ảnh hưởng tiêu cực đến tính *bảo mật, tính toàn vẹn, tính khả dụng* của dữ liệu hoặc hệ thống máy tính (UNODC, 2013). Nói một cách đơn giản, thông tin cá nhân phải ở chế độ riêng tư, không được thay đổi nếu không có sự cho phép của chủ sở hữu và dịch vụ và hệ thống giúp chủ sở hữu truy cập dữ liệu mọi lúc. Tội phạm này có các hành vi đặc trưng như tấn công mạng, gián điệp mạng. Trong đó *"Tấn công mạng"* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử... *"Gián điệp mạng"* là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng

Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của cơ quan, tổ chức, cá nhân. Khi ICT là phương thức hỗ trợ hành vi phạm tội thì tính nguy hiểm của hành vi phạm tội chính là tính nguy hiểm của tội phạm truyền thống mà thông qua ICT để thực hiện. Ví dụ: hành vi sử dụng Internet, các công nghệ kỹ thuật số để lừa đảo, trộm cắp, khủng bố, tài trợ khủng bố...

– Tội phạm mạng có thể được thực hiện bởi các cá nhân hay tổ chức với các động cơ, mục đích, phương thức, thủ đoạn khác nhau. Ví dụ: Sử dụng phần mềm độc hại tấn công hệ thống máy tính, chúng có động cơ và mục đích khác nhau để thực hiện tội phạm mạng.

– Tội phạm mạng có phạm vi và ảnh hưởng lớn đến xã hội, có khả năng tác động toàn cầu như khả năng bao trùm và ảnh hưởng của mạng Internet, mạng viễn thông.

– Tương tự như tội phạm mạng, tội phạm công nghệ cao cũng bắt buộc có công nghệ cao, đây là đối tượng tấn công của hành vi phạm tội hoặc sử dụng công nghệ cao để thực hiện hành vi phạm tội truyền thống khác.

1.3. Phân loại tội phạm mạng, tội phạm sử dụng công nghệ cao

Mặc dù vẫn tồn tại nhiều cách hiểu khác nhau, nhưng về cơ bản khái niệm tội phạm mạng, tội phạm sử dụng công nghệ cao nhưng về nội hàm của khái niệm về cơ bản được thống nhất với nhau và có thể phân thành hai loại đó là:

Thứ nhất: Nhóm tội phạm có mục tiêu tấn công, tác động trực tiếp hoặc gián tiếp vào sự hoạt động bình thường và phát triển của công nghệ cao, của máy tính, mạng máy tính, các thiết bị ngoại vi, các cơ sở dữ liệu, các quá trình điều khiển dựa trên sự hoạt động của các thiết bị tin học; tấn công hạ tầng thông tin quốc gia, cơ sở dữ liệu của các cơ quan nhà nước và doanh nghiệp; phát tán vi rút, chương trình tin học có tính năng gây hại, phần mềm gián điệp... để can thiệp phá hoại, chiếm đoạt quyền điều khiển, trộm cắp thông tin dữ liệu...

Hình thức thể hiện của nhóm này như các hành vi vượt qua tường lửa, mật khẩu (password), cảnh báo để truy cập bất hợp pháp vào cơ sở dữ liệu nhằm phá hoại, sửa đổi, trộm cắp dữ liệu, sử dụng trái phép thông tin trộm cắp, tấn công từ chối dịch vụ (DOSS, BOTNET), phát tán vi rút, phần mềm gián điệp, thư rác...

Thứ hai: Nhóm tội phạm sử dụng phương tiện kỹ thuật số, mạng máy tính, mạng viễn thông, mạng Internet, công nghệ điện toán đám mây, trí tuệ nhân tạo, Internet vạn vật, công nghệ sinh học phân tử, công nghệ vật liệu mới, công nghệ hóa học… để làm công cụ để thực hiện các hành vi phạm tội mang tính "truyền thống" trong các lĩnh vực của đời sống xã hội. Điển hình của nhóm này như các hành vi: lừa đảo qua mạng internet, mạng viễn thông, trộm cắp tiền từ thẻ tín dụng; đánh bạc; cá độ bóng đá; rửa tiền; buôn bán ma tuý; tuyên truyền văn hoá phẩm đồi truỵ; môi giới mại dâm; xâm phạm quyền sở hữu trí tuệ; khủng bố; quấy rối; xúc phạm danh dự nhân phẩm người khác... qua mạng.

– Trên cơ sở các quy định của Bộ luật hình sự (BLHS) năm 2015 có thể phân loại tội phạm mạng thành các dạng sau:

+ Hành vi tấn công làm ảnh hưởng trực tiếp đến mạng máy tính, mạng viễn thông (10 Điều luật tại Chương XXI). Trong đó, BLHS sửa đổi năm 2017 đã phi hình sự hóa hành vi quy định tại Điều 292 tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông BLHS 2015.

+ Hành vi sử dụng mạng máy tính, mạng viễn thông là công cụ, phương tiện phạm tội là tình tiết định khung tăng nặng (Điều 155 tội làm nhục người khác; Điều 156 tội vu khống, Điều 321 tội đánh bạc…).

+ Các tội phạm truyền thống có sử dụng mạng máy tính, mạng viễn thông khi thực hiện tội phạm (Khiến tính chất, mức độ của hành vi phạm tội nguy hiểm hơn).

2. Chứng cứ điện tử trong việc phát hiện và xử tội phạm mạng, tội phạm công nghệ cao

2.1. Chứng cứ và chứng minh trong giải quyết vụ án hình sự liên quan đến tội phạm mạng, tội phạm sử dụng công nghệ cao

Điều 86 Bộ luật tố tụng hình sự Việt Nam năm 2015 quy định về chứng cứ như sau: *"Chứng cứ là những gì có thật, được thu thập theo trình tự, thủ tục do Bộ luật Tố tụng hình sự quy định, được dùng làm căn cứ để xác định có hay không hành vi phạm tội, người thực hiện hành vi phạm tội và những tình tiết khác có ý nghĩa trong việc giải quyết vụ án." (Điều 86 Bộ Luật tố tụng hình sự Việt Nam, 2015).*

Như vậy, chứng cứ là những thông tin có ý nghĩa đối với quá trình giải quyết vụ án, đảm bảo tính hợp pháp, tính liên quan, tính khách quan thì được coi là chứng cứ và dùng làm căn cứ để giải quyết vụ án hình sự. Chứng cứ thì được chứa đựng từ các nguồn khác nhau có thể là: *Vật chứng, lời khai, lời trình bày, dữ liệu điện tử…* (Điều 87 Bộ Luật tố tụng hình sự Việt Nam, 2015) Có thể thấy rằng, pháp luật tố tụng hình sự Việt Nam 2015 lần đầu tiên công nhận dữ liệu điện tử là nguồn của chứng cứ và được sử dụng để làm căn cứ quan trọng trong quá trình giải quyết vụ án hình sự. Tuy nhiên, ở Việt Nam trình tự, thủ tục để bảo quản, thu thập đối với chứng cứ điện tử chưa được quy định riêng, mà chỉ được công nhận khi bảo đảm được các đặc trưng cơ bản của chứng cứ nói chung.

Trong lĩnh vực công nghệ thông tin thì dấu vết điện tử là kết quả để lại của việc sử dụng công nghệ thông tin và truyền thông của cá nhân. Đặc biệt, một người khi sử dụng công nghệ thông tin và truyền thông có thể để lại dấu vết mang thông tin của họ bao gồm: Độ tuổi, giới tính, dân tộc, quốc tịch, sở thích, suy nghĩ, thói quen.... Thông tin này có thể do chính người dùng cố ý hoặc vô ý để lại thông qua thông tin cá nhân mà người dùng cung cấp, hình ảnh, video, bình luận, nhận xét... việc để lại thông tin này có thể được dùng làm chứng cứ buộc tội một người hoặc có thể sử dụng nó để bác bỏ hoặc ủng hộ một quan điểm buộc tội, loại trừ những chủ thể không thực hiện hành vi phạm tội.

Các dữ liệu này được lưu trữ trên các thiết bị kỹ thuật số như: Máy tính, điện thoại thông minh, máy tính bảng, ổ cứng, USB... hoặc bất kỳ các thiết bị nào có khả năng lưu trữ dữ liệu. Các dữ liệu này có thể là dữ liệu trực tiếp chứng minh tội phạm như: Tin nhắn bằng văn bản, video, ghi âm và là dữ liệu gián tiếp để chứng minh tội phạm như: Thông tin của người gửi và người nhận, danh tính và vị trí của người đã sử dụng dữ liệu hoặc giao dịch.

Dữ liệu thu được trực tuyến hoặc trích xuất từ các thiết bị lưu trữ khác có thể cung cấp nhiều thông tin về người dùng và nội dung mà nó hàm chứa. Ví dụ như: lưu trữ thông tin về người dùng thiết bị, thông tin tài chính, lịch sử trình duyệt Web... Một số phần mềm có thể cung cấp thông tin về người dùng như chủ sử hữu, sở thích, truy vấn mua hàng và đánh cắp các hoạt động vị trí mà người dùng đã lưu đến. Thông qua các phần mềm này giúp cho cơ quan tiến hành tố tụng dễ dàng trong việc tìm ra đối tượng thực hiện hành vi phạm tội.

Cũng giống như đặc trưng cơ bản của chứng cứ, trước khi một dữ liệu điện tử có thể được coi là chứng cứ điện tử và có giá trị trong việc chứng minh tội phạm thì nó phải được đảm bảo bởi yếu tố khách quan, nó tồn tại không phụ thuộc vào ý thức chủ quan

của con người, chưa bị tác động vào sau khi kết thúc sự kiện tội phạm xảy ra và được thu thập theo đúng trình tự, thủ tục mà Bộ luật tố tụng hình sự quy định (Nguyễn Đức Hạnh, Lại Viết Quang, 2021).

Khi so sánh giữa chứng cứ vật chất và chứng cứ điện tử đặt ra những thách thức cho cơ quan tiến hành tố tụng về việc bảo quản chứng cứ điện tử, tính dễ bị đánh cắp, biến mất hoặc bị thay đổi. Trên thế giới, một số quốc gia đã đưa ra các quy chuẩn tố tụng trong việc bảo quản, lưu trữ, trích xuất riêng biệt đối với chứng cứ điện tử, còn một số quốc gia khác thì quy định tương tự việc bảo quản, lưu trữ chứng cứ điện tử giống như chứng cứ vật chất khác. Ví dụ ở Pháp, cả chứng cứ vật chất và chứng cứ điện tử đều phải xác thực bằng cách xác minh danh tính của người phát hiện, cung cấp chứng cứ trên hoặc tính nguyên vẹn chưa bị tác động của chứng cứ. Loại thứ hai không chỉ đề cập đến độ chính xác của chứng cứ điện tử mà còn là khả năng duy trì độ chính xác của nó theo thời gian, đối với một số loại chứng cứ điện tử ở một số thời điểm nhất định chúng có độ tin cậy và chính xác cao, tuy nhiên, sau một thời gian mà chúng được biến đổi theo thuật toán hoặc sự ảnh hưởng của nhà cung cấp, dẫn đến sai lệch về tính chính xác. Ở Singapore đã sửa đổi Đạo luật về Bằng chứng (2012) để bảo đảm cho việc xác định chứng cứ điện tử giống như chứng cứ vật chất thông thường (Nguyễn Đức Hạnh, Lại Viết Quang, 2021).

Ngoài việc xác định tính xác thực của chứng cứ điện tử thì ở một số quốc gia cũng kiểm tra xem chứng cứ đó có được sao lưu hoặc đồng nhất với chứng cứ gốc hay không, chưa bị sửa đổi hoặc bị tác động bởi con người và đã được tòa án công nhận. Hơn nữa, việc đánh giá tính xác thực của chứng cứ cũng liên quan đến quy trình, thủ thục để thu thập, bảo quản, phân tích dữ liệu điện tử, đảm bảo rằng dữ liệu này không bị sửa đổi, bổ sung theo bất kỳ hình thức nào.

2.2. Đặc điểm chứng cứ điện tử trong các vụ án liên quan đến tội phạm sử dụng công nghệ cao

Thứ nhất, chứng cứ điện tử chỉ được thu thập, xác định từ nguồn "dữ liệu điện tử" nên ngoài các thuộc tính của chứng cứ (tính khách quan, tính liên quan và tính hợp pháp), thì chứng cứ điện tử còn có những đặc điểm gắn liền với bản chất, hình thức và đặc tính của dữ liệu điện tử.

Tại Điều 99 BLTTHS quy định: *"1. Dữ liệu điện tử là ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được tạo ra, lưu trữ, truyền đi hoặc nhận được bởi phương tiện điện tử; 2. Dữ liệu điện tử được thu thập từ phương tiện điện tử, mạng máy tính, mạng viễn thông, trên đường truyền và các nguồn điện tử khác…".*

Như vậy, bản chất của dữ liệu điện tử là những thông tin thể hiện dưới dạng tín hiệu điện tử như: các ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc những dạng tương tự. Các nguồn lưu trữ dữ liệu điện tử bao gồm: phương tiện điện tử, mạng máy tính, mạng viễn thông, đường truyền và các nguồn điện tử khác. Có nghĩa, dữ liệu điện tử có thể tồn tại, lưu trữ trong các vật thể cụ thể (các phương tiện điện tử có bộ nhớ kỹ thuật số như: máy tính, mạng máy tính, điện thoại di động, ổ cứng di động, đĩa quang…) nhưng cũng có thể tồn tại trong không gian lưu trữ khác (như: email, website, account của đối tượng, server của nhà cung cấp dịch vụ Internet, điện toán đám mây (Viện Tiêu chuẩn và Công nghệ Mỹ - NIST, 2022)...

Dữ liệu điện tử có thể được hình thành theo các cơ chế sau:

+ Dữ liệu điện tử do máy tính tự động tạo ra: Đây là kết quả được tạo ra sau khi chương trình máy tính xử lý các dữ liệu đầu vào theo một thuật toán đã được xác định.

Ví dụ, nhật ký truyền tệp tin trong máy tính (FTP tranfer logs); các bản ghi định vị (GPS records); các bản ghi và nhật ký trang thư điện tử (Web mail logs IP logs and records); thông tin truy cập website… Những dữ liệu này có giá trị chứng minh về nguồn gốc truy cập, địa chỉ tấn công vào website, cơ sở dữ liệu, dấu vết hoạt động phạm tội (như: hành vi truy cập trái phép, tấn công DDOS, cài trojan, keylogger, sniffer nghe lén, lấy cắp hoặc phá hoại dữ liệu...).

+ Dữ liệu điện tử do con người tạo ra: Đây là những thông tin điện tử do người sử dụng tạo ra, được lưu giữ trong máy tính hoặc các thiết bị điện tử khác. Ví dụ, các văn bản, bảng biểu, các hình ảnh, thông tin người sử dụng các dịch vụ, nội dung các cuộc trò chuyện trên mạng… được lưu giữ dưới dạng tín hiệu điện tử, có giá trị chứng minh về máy tính, người đã tạo ra dữ liệu, nguồn gốc dữ liệu. Vì vậy, khi các dữ liệu này được khởi tạo, lưu giữ, truyền đi và nhận lại một cách khách quan, nội dung có chứa các thông tin liên quan đến hành vi phạm tội, người thực hiện tội phạm và được thu thập theo trình tự, thủ tục do BLTTHS quy định thì được xác định là chứng cứ.

+ Dữ liệu điện tử có các đặc tính: Hình thành tự động dưới dạng tín hiệu số; thời gian tồn tại có giới hạn, phụ thuộc vào thiết bị, phần mềm lưu trữ và hành vi, thói quen của người sử dụng; dễ bị tác động, bị xóa hoặc thay đổi trong quá trình lưu trữ, truyền tải, sao chép,… bởi các yếu tố tác động như: vi rút, dung lượng bộ nhớ, lệnh lưu trữ của phần mềm, phương pháp truy cập, mở, mã hóa, sao lưu, việc cố ý hoặc vô ý sửa đổi, xóa bỏ dữ liệu... Tuy nhiên, dữ liệu điện tử lại có thể được phục hồi, phân tích, giải mã sau khi bị xoá bỏ, bị mã hoá, ghi đè,…; trong các vụ án về tội phạm công nghệ cao, các đối tượng phạm tội thường sử dụng phần mềm công nghệ cao để mã hóa dữ liệu hoặc dễ dàng tiêu hủy các thiết bị lưu trữ dữ liệu khi bị phát hiện, nhất là gây ra những hỏng hóc về mặt vật lý để che giấu chứng cứ phạm tội. Việc này làm cho công tác tìm kiếm, phục hồi, giám định dữ liệu điện tử gặp khó khăn. Nhưng khi dữ liệu điện tử đã được các chuyên gia giám định, phục hồi, giải mã, phân tích và chuyển hóa thành các dạng thông tin có thể ghi lại, đọc được hoặc nhìn thấy được thì có giá trị sử dụng làm chứng cứ chứng minh tội phạm.

Thứ hai, để trở thành chứng cứ, dữ liệu điện tử phải đáp ứng đầy đủ các thuộc tính là tính khách quan, tính hợp pháp và tính liên quan của chứng cứ. Cụ thể là:

- Dữ liệu điện tử là có thật, tồn tại khách quan, có nguồn gốc rõ ràng, không bị làm sai lệch, biến dạng; đã được tìm thấy và đang lưu trên máy tính, điện thoại di động, máy tính bảng, USB, email, tài khoản trên mạng, trên máy chủ của nhà cung cấp dịch vụ Internet, điện toán đám mây...

– Dữ liệu điện tử phải được thu thập một cách hợp pháp, đòi hỏi việc thu thập, bảo quản dữ liệu điện tử phải được thực hiện đúng quy định của BLTTHS. Bởi vì, những gì có thật, mang dấu vết của tội phạm nhưng không được thu thập, bảo quản theo trình tự, thủ tục do BLTTHS quy định thì không có giá trị pháp lý và không được dùng làm căn cứ để giải quyết vụ án hình sự (khoản 2 Điều 87 BLTTHS, 2015). Do đó, trong cả quá trình khám xét, thu giữ phương tiện điện tử, sao lưu dữ liệu, chặn thu trên đường truyền, bảo quản, phục hồi, phân tích, tìm kiếm và giám định dữ liệu phải sử dụng công nghệ phù hợp, được pháp luật công nhận.

– Dữ liệu điện tử phải liên quan đến việc giải quyết vụ án, phản ánh những thông tin về sự việc phạm tội, giúp xác định hành vi phạm tội, người phạm tội và những tình tiết khác có ý nghĩa đối với việc giải quyết vụ án.

Thứ ba, giữa dữ liệu điện tử và chứng cứ điện tử có mối liên hệ mật thiết. Chứng cứ điện tử chỉ có thể khai thác từ nguồn dữ liệu điện tử nhưng chỉ dữ liệu điện tử nào đảm bảo đầy đủ các thuộc tính của chứng cứ thì mới trở thành chứng cứ chứng minh trong vụ án hình sự. Trong một số trường hợp, có thể thu được các dữ liệu điện tử nhưng do cách thức khởi tạo, lưu trữ, truyền gửi dữ liệu không đảm bảo tính khách quan, nguyên vẹn, làm cho dữ liệu điện tử không phản ánh đúng bản chất của sự vật, hiện tượng hoặc dữ liệu điện tử không được thu thập, bảo quản theo đúng trình tự, thủ tục mà BLTTHS quy định.

Thứ tư, khi tìm kiếm, phát hiện thu giữ chứng cứ điện tử từ nguồn dữ liệu điện tử phải chú ý những đặc điểm cơ bản như: Dữ liệu điện tử có tính biến đổi, có thể bị xóa, bị chỉnh sửa hoặc bị phá hủy nhưng có thể được phục hồi sau khi bị xoá bỏ; dữ liệu điện tử không nhìn thấy bằng mắt thường, luôn gắn với thiết bị điện tử hoặc phương tiện điện tử nhất định; có thể được tạo ra trong không gian và không có tính biên giới, lãnh thổ; có thuộc tính sao chép (copy) y nguyên và bản sao của nó có thể được sử dụng cho mục đích kiểm tra; có thể dễ dàng xác định là chứng cứ đã được thay đổi hoặc giả mạo.

Thứ năm, cũng như mọi hành vi phạm tội "truyền thống", tội phạm sử dụng công nghệ cao cũng để lại dấu vết mang tính vật chất. Đó là những "dữ liệu điện tử" tồn tại khách quan trong quá trình thực hiện tội phạm, dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh hoặc âm thanh hoặc dạng tương tự. Điểm khác biệt so với tội phạm "truyền thống", đó là môi trường tồn tại của chứng cứ. Nếu như ở tội phạm "truyền thống", những "dấu vết, vật chứng" phản ánh hành vi phạm tội luôn tồn tại trong một không gian "thực" - (một địa điểm cụ thể nào đó) và trong một khoảng thời gian nhất định, thì "dấu vết" trong tội phạm công nghệ cao được lưu giữ trong máy tính hoặc các thiết bị có bộ nhớ kỹ thuật số khác. Đặc điểm của những "dữ liệu" hay "tín hiệu điện tử" này là chúng được tạo ra một cách tự động, khách quan (độc lập với ý chí của thủ phạm), và được lưu giữ trong máy tính hoặc các thiết bị số một cách tự động. Nơi lưu giữ chúng là bộ nhớ của "phương tiện điện tử". (Phương tiện điện tử là phương tiện hoạt động dựa trên công nghệ điện, điện tử, kỹ thuật số, từ tính, truyền dẫn không dây, quang học, điện từ hoặc công nghệ tương tự - Điều 4, Luật Giao dịch điện tử 2005). Những dữ liệu này tồn tại trong một thời gian nhất định (phụ thuộc vào phần mềm được cài đặt sẵn).

"Dữ liệu điện tử" được biểu hiện bằng "Thông điệp điện tử" có khả năng truyền tài thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự được nhận và được lưu trữ bằng phương tiện điện tử (như chứng từ điện tử, thư điện tử, điện tín, điện báo, fax và các hình thức tương tự khác…). Giá trị chứng cứ của "thông điệp dữ liệu" được xác định căn cứ vào độ tin cậy của cách thức khởi tạo, lưu trữ hoặc truyền gửi, cách thức bảo đảm và duy trì tính toàn vẹn, cách thức xác định người khởi tạo...

3. Những vấn đề đặt ra đối với hoạt động đào tạo ngành luật trong các trường đại học ở Việt Nam hiện nay

3.1. Một số thách thức hiện nay liên quan đến tội phạm mạng, tội phạm công nghệ cao

3.1.1. Thách thức về kỹ thuật

Đối với hoạt động phòng ngừa và chống các loại tội phạm mạng, tội phạm công nghệ cao giai đoạn hiện nay gặp phải những khó khăn về mặt kỹ thuật như:

– Một máy tính nào được kết nối với Internet đều có thể giao tiếp với bất kỳ máy tính nào khác cũng được kết nối với Internet. Thông thường, để xác định được tội phạm chúng ta thường dựa vào địa chỉ IP của máy tính, địa chỉ IP này có tác dụng truy nguyên

ra máy tính khi máy tính đó kết nối với máy tính khác. Thông qua địa chỉ IP cho phép xác định vị trí tội phạm sử dụng máy tính ở quốc gia nào, nhà cung cấp dịch vụ Internet nào cung cấp dịch vụ cho máy tính của tội phạm. Tuy nhiên, với công nghệ hiện nay nhiều tội phạm đã biết cách làm ẩn địa chỉ IP khi thực hiện tội phạm, hoặc giả vờ đang kết nối từ một địa chỉ IP khác (tạo ra một địa chỉ IP ảo), sử dụng nhiều công cụ khác nhau để che khuất quyền truy cập… nhằm trốn tránh sự phát hiện của các cơ quan thực thi pháp luật.

– Ngày nay các phần mềm giúp chúng ta sử dụng được các ứng dụng trên máy tính, điện thoại, thông qua phần mềm mới có thể truy cập được các Websites. Tuy nhiên, các phần mềm thường có những *"lỗ hổng bảo mật"*. Nguyên nhân của các lỗ hổng bảo mật có thể là sự cố trong chương trình hoặc cấu hình sai khi xây dựng chương trình… Với các lỗ hổng bảo mật này cho phép kẻ phạm tội tấn công mạng máy tính, can thiệp vào hệ thống, lấy cắp thông tin như tải xuống thông tin thẻ tín dụng của khách hàng, mật khẩu, email...

– Thực tiễn thời gian qua cho thấy một số Công ty phần mềm không kịp thời phát hiện ra các lỗ hổng từ các phần mềm mà họ sản xuất ra, những lỗ hổng thường xuất hiện liên quan đến những phần mềm lớn, thường xuyên thay đổi, cập nhật. Mặt khác, những đối tượng phạm tội khi phát hiện ra lỗ hổng của các phần mềm mà chưa được khắc phục đã khai thác đặc điểm khi có lỗ hổng phần mềm thì các chương trình diệt vi-rút không thể phát huy tác dụng chống lại vi-rút (mã độc) nên các đối tượng này dễ dàng tấn công mạng máy tính khai thác các thông tin bảo mật, các dữ liệu của người dùng. Ví dụ: Năm 2017, Equifax - một dịch vụ báo cáo tín dụng của Hoa Kỳ - đã mất "dữ liệu cá nhân nhạy cảm" của 143 triệu người dân Mỹ vì một lỗ hổng phần mềm (Timberg, Craig, Elizabeth Dowskin, Brian Fung, 2017). Lỗ hổng này đã bị các đối tượng phạm tội khai thác trong ba tháng mới được khắc phục. Việc mất dữ liệu từ các lỗ hổng phần mềm là tương đối phổ biến, ngay cả đối với các tổ chức lớn vì rất khó khi tạo cấu hình, bảo mật các hệ thống kỹ thuật số đúng cách.

– Một thách thức về phương diện kỹ thuật khác liên quan đến cơ sở hạ tầng công nghệ thông tin ảo hóa (ví dụ: đám mây). Khi cơ sở dữ liệu của một cá nhân, tổ chức được chuyển vào đám mây thì các dữ liệu chỉ an toàn, toàn vẹn khi các nhà cung cấp dịch vụ đám mây đó có đầy đủ khả năng và trách nhiệm an ninh đối với đám mây (ví dụ: bảo mật hệ thống vật lý, bảo mật trung tâm dữ liệu). Tuy nhiên việc đảm bảo an ninh đối với đám mây không phải lúc nào cũng an toàn trước sự tấn công của tội phạm mạng.

3.1.2. Thách thức về khung pháp lý

Tội phạm mạng, công nghệ cao đa phần đều là loại tội phạm xuyên quốc gia do vậy đối tượng phạm tội cũng như nạn nhân có thể ở bất kỳ đâu trên thế giới miễn là nơi đó có kết nối Internet. Do đó, để có thể phát hiện và xử lý loại tội phạm này thì quá trình điều tội phạm mạng các cơ quan chức năng cũng thường yêu cầu quyền truy cập và chia sẻ dữ liệu xuyên biên giới. Điều này chỉ có thể thực hiện được nếu các nhà cung cấp dịch vụ lưu giữ đầy đủ dữ liệu và cho phép các cơ quan thực thi pháp luật truy cập vào dữ liệu đó. Tuy nhiên, do pháp luật của mỗi quốc gia là khác nhau về các thủ tục tố tụng hình sự như việc thu thập chứng cứ, chứng minh và xử lý tội phạm… khả năng thực hiện các điều ước quốc tế về phòng, chống tội phạm mạng, tội phạm công nghệ cao, tội phạm xuyên quốc gia là khác nhau và những quy định về bảo vệ thông tin cá nhân, nhân quyền cũng khác nhau. Đây là những thách thức pháp lý chính đối với việc phát hiện, điều tra, truy tố, xét xử tội phạm mạng.

3.1.3. Thách thức về khía cạnh đạo đức

Khi điều tra các tội phạm mạng, tội phạm công nghệ cao các cơ quan chức năng, cơ quan tố tụng phải truy cập vào các cơ sở dữ liệu của cá nhân người dùng, của người bị

hại, của các đối tượng phạm tội… Như vậy, để tiếp cận được những thông tin có ý nghĩa trong việc chứng minh tội phạm thì họ cũng tiếp cận và biết được rất nhiều các thông tin khác, trong đó có cả những thông tin riêng tư thuộc về bí mật của riêng họ. Nếu những người thực thi pháp luật, những người có trách nhiệm trong các cơ quan tố tụng không có đạo đức công vụ tốt thì có thể những thông tin mà họ biết được sẽ làm hại đối với người bị hại một lần nữa, cũng như làm ảnh hưởng đến quyền và lợi ích của các tổ chức, cá nhân có liên quan.

Để các cá nhân sử dụng hệ thống máy tính có thể truy cập và sử dụng các ứng dụng phần mềm do các nhà cung cấp dịch vụ hoặc công ty sản xuất phần mềm tạo ra, khi đăng ký sử dụng phần mềm, dịch vụ cung cấp người dùng thường phải cam kết đồng ý tự nguyện tham gia hoặc phải cung cấp những thông tin cá nhân. Nếu các nhà cung cấp dịch vụ không đề cao đạo đức kinh doanh thì những thông tin cá nhân của người dùng dịch vụ có thể bị lọt ra ngoài ảnh hưởng đến quyền và lợi ích hợp pháp của người dùng. Việc đánh giá dưới góc độ đạo đức xã hội về hành vi nhân bản vô tính thực vật, động vật và người có nhiều cách nhìn nhận, đánh giá rất khác nhau, thậm trí còn trái ngược nhau.

3.1.4. Thách thức trong việc hợp tác giữa các quốc gia

Hoạt động điều tra tội phạm mạng, tội phạm công nghệ cao thường liên quan đến nhiều quốc gia khác nhau nên rất cần sự hợp tác quốc tế, dẫn độ tội phạm và tương trợ tư pháp hình sự giữa các quốc gia. Tuy nhiên, giữa các quốc gia không phải lúc nào cũng có các hiệp định tương trợ tư pháp ký kết song phương với các quốc gia khác hoặc tham gia các điều ước đa phương về tương trợ tư pháp nên khi điều tra các tội phạm mạng có yếu tố nước ngoài, các cơ quan tố tụng phải thông qua con đường ngoại giao để thực hiện đối với việc tương trợ, dẫn đến thời gian thường kéo dài, đôi khi không có kết quả hoặc kết quả không được như mong muốn. Đối với những quốc gia đang phát triển và kém phát triển thì nguồn lực để thực hiện việc tương trợ tư pháp là rất hạn chế dẫn đến việc phát hiện, xử lý tội phạm mạng, tội phạm công nghệ cao còn gặp nhiều khó khăn.

3.2. Hoạt động đào tạo ngành luật trong các trường đại học ở Việt Nam trước những thách thức liên quan đến tội phạm mạng, tội phạm công nghệ cao

Với những phân tích trên đây, chúng tôi cho rằng hoạt động đào tạo ngành luật trong các trường đại học ở Việt Nam trước những thách thức liên quan đến tội phạm mạng, tội phạm công nghệ thông tin phải chú trọng các nội dung sau:

– Nên chú trọng và triển khai triệt để việc thiết kế và chuyển đổi chương trình đào tạo theo niên chế sang theo tín chỉ giúp sinh viên không bị hạn chế trong việc lựa chọn giảng viên, việc phân bổ giờ lý thuyết, giờ thực hành, giờ thảo luận, giờ tự học...

– Xây dựng giáo trình điện tử về tội phạm mạng, tội phạm công nghệ cao kết hợp hình thức học viên nghiên cứu giáo án điện tử trước, giáo viên trên lớp chủ yếu mở rộng kiến thức và thảo luận, định hướng cho sinh viên.

– Nâng cao trình độ tiếng Anh của giáo viên, sinh viên để có thể nghiên cứu học tập, giảng dạy và tham khảo bằng tiếng Anh, tận dụng được các tri thức và khoa học công nghệ hiện đại là thành tựu của thế giới và của cuộc cách mạng khoa học công nghệ 4.0.

– Xây dựng đội ngũ giảng viên có kiến thức và kinh nghiệm thực tế, chuyên sâu về tội phạm mạng, tội phạm công nghệ cao.

– Triển khai khả năng hội nhập quốc tế và tương tác với các trường đại học trên thế giới trong việc tiếp thu vận dụng tri thức, thành tựu của cuộc cách mạng công nghiệp 4.0 trong giảng dạy thông qua việc trao đổi sinh viên, giảng viên.

– Xây dựng thư viện số, thư viện điện tử của từng trường đại học và có liên kết thành mạng lưới các trường đại học, liên kết với thư viện số của thư viện quốc gia.

– Trong chương trình đào tạo luật phải được bổ sung các môn học có mục tiêu cung cấp tri thức, kỹ năng cho người học về công nghệ số, người máy thông minh, không gian mạng, tư liệu điện tử, an ninh mạng, trí tuệ nhân tạo, ứng dụng công nghệ thông tin, tài nguyên số, sở hữu trí tuệ, công nghệ sinh học phân tử, tự động hóa...

– Khi thiết kế chương trình và môn học luật phải đảm bảo điều kiện cho người học tương tác với thực tiễn công việc và gắn với thực tiễn hoạt động thực hành nghề luật. Kết hợp với các cơ quan tư pháp, cơ quan, đơn vị sử dụng lao động từ các cơ sở đào tạo luật để các sinh viên, học viên có cơ hội thực hành cao, thực hành thông qua tương tác điện tử, mạng Internet...

– Sử dụng ứng dụng khoa học kỹ thuật để tổ chức khảo thí và kiểm định chất lượng đào tạo đảm bảo công bằng, khách quan đối với các phần học, môn học.

– Chú trọng đào tạo các môn học chuyên sâu về đạo đức nghề nghiệp, các môn học thuộc về lĩnh vực liên quan nhiều đến thương mại điện tử, tư pháp quốc tế...

– Tăng cường nghiên cứu khoa học với những chủ đề về tội phạm mạng, tội phạm công nghệ cao, chứng cứ điện tử.

– Chú trọng đào tạo để trang bị kiến thức cho sinh viên liên quan đến tài phán đối với các tội phạm sự dụng mạng bưu chính, mạng viễn thông để phạm tội xuyên quốc gia với những trường hợp thực hiện tội phạm ở nước này với các bị hại ở nước khác bằng việc sử dụng nhà cung cấp dịch vụ ở nước thứ ba; kiến thức về phục hồi dữ liệu điện tử bị xóa, thu thập dữ liệu điện tử trên đường truyền, trên mạng Internet, Icloud, trong các phần mềm; quy định việc sử dụng trí tuệ nhân tạo để phát hiện, thu thập chứng cứ, bảo quản, đánh giá và sử dụng dữ liệu điện tử cần có những khung pháp lý cụ thể…

TÀI LIỆU THAM KHẢO

[1] Group 1 (2009). *Issues and measure concerning the legal framework to combat cybercrime*. Resource Material series No. 79, UNAFEI.

[2] Nguyễn Đức Hạnh, Lại Viết Quang đồng chủ biên, (2021). *Tội phạm mạng máy tính và công nghệ thông tin, truyền thông.* NXB Thanh Niên, Hà Nội

[3] Quốc hội (2015). Bộ luật Hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam. Số: 100/2015/QH13, ngày 27 tháng 11 năm 2015.

[4] Quốc hội (2015). Bộ luật Tố tụng dân sự nước Cộng hòa xã hội chủ nghĩa Việt Nam. Luật số: 92/2015/QH13, ngày 25 tháng 11 năm 2015.

[5] Quốc hội (2015). Bộ luật Tố tụng Hình sự nước Cộng hòa xã hội chủ nghĩa Việt Nam. Luật số: 101/2015/QH13, ngày 27 tháng 11 năm 2015.

[6] Quốc hội (2015). Luật tố tụng hành chính nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2015. Luật số: 93/2015/QH13, ngày 25 tháng 11 năm 2015.

[7] Quốc hội (2023). Luật giao dịch điện tử nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2023. Luật số: 20/2023/QH15, ngày 22 tháng 6 năm 2023.

[8] Tài liệu hội thảo *"Tập huấn điều tra tội phạm trên không gian mang"*. Viện Kiểm sát Nhân

[9] Timberg, Craig, Elizabeth Dowskin, Brian Fung (2017). Data of 143 million Americans exposed in hack of credit reporting agency Equifax. *The Washington Post*.